УДК 681.3.06
Дудикевич В.Б ., Томашевський Б.П.

ДОСЛІДЖЕННЯ МЕХАНІЗМІВ КОМПЛЕКСНОГО ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ І ДОСТОВІРНОСТІ ПЕРЕДАЧІ ДАНИХ В КОМП'ЮТЕРНИХ СИСТЕМАХ І МЕРЕЖАХ

1. Постановка проблеми в загальному вигляді і аналіз літератури. Проблема захисту комп'ютерних мереж і систем від несанкціонованого доступу в сучасних умовах набула особливу гостроту. Стрімкий розвиток комунікаційних технологій дозволяє будувати мережі розподіленої архітектури, що об'єднують велику кількість сегментів, розташованих на значній відстані один від одного. Усе це викликає збільшення числа вузлів мереж і кількості різних ліній зв'язку між ними, що, у свою чергу, підвищує ризик несанкціонованого підключення до мережі і доступу до важливої інформації [1-3].

Збільшення об'ємів даних, які оброблюються і передаються, в комп'ютерних системах і мережах, передусім в банківських системах, в системах управління великими фінансовими і промисловими організаціями, підприємствами енергетичного сектору, транспорту, в системах управління і зв'язку військового призначення вимагає нових підходів в організації протоколів і механізмів забезпечення безпеки даних, які передаються. Вимога до безпеки і достовірності інформації, яка оброблюється і передається, в таких системах стоїть дуже гостро, оскільки відмова системи або вихід за встановлені обмеження вказаних параметрів може привести до значних фінансових і матеріальних втрат, зниження обороноздатності країни, збитку екології, життя і здоров'я людей.

Проведений аналіз показує [1-6], що за останній час загальний об'єм інформації, яка оброблюється і передається в комп'ютерних системах і мережах зріс багаторазово (на два-три порядки зростає кожні п’ять-десять років) і загальні тенденції свідчать, що така динаміка збережеться. Сучасні криптографічні засоби захисту інформації в таких умовах повинні забезпечувати своєчасну обробку величезних об'ємів даних (десятки-сотні Мбіт/с) і задовольняти жорстким вимогам по достовірності і безпеці інформації.

Метою цієї статті є дослідження механізмів комплексного забезпечення безпеки і достовірності передачі даних в комп'ютерних системах і мережах, обґрунтування перспективних шляхів якісного вдосконалення методів і обчислювальних алгоритмів захисту інформації.

2. Дослідження механізмів захисту інформації в комп'ютерних системах і мережах. Механізми забезпечення безпеки інформації в комп'ютерних системах і мережах в більшості засновані на криптографічних методах, загальна класифікація яких приведена на рис. 1. Це методи симетричної і несиметричної криптографії, розвитку яких присвячені численні роботи [1-11].

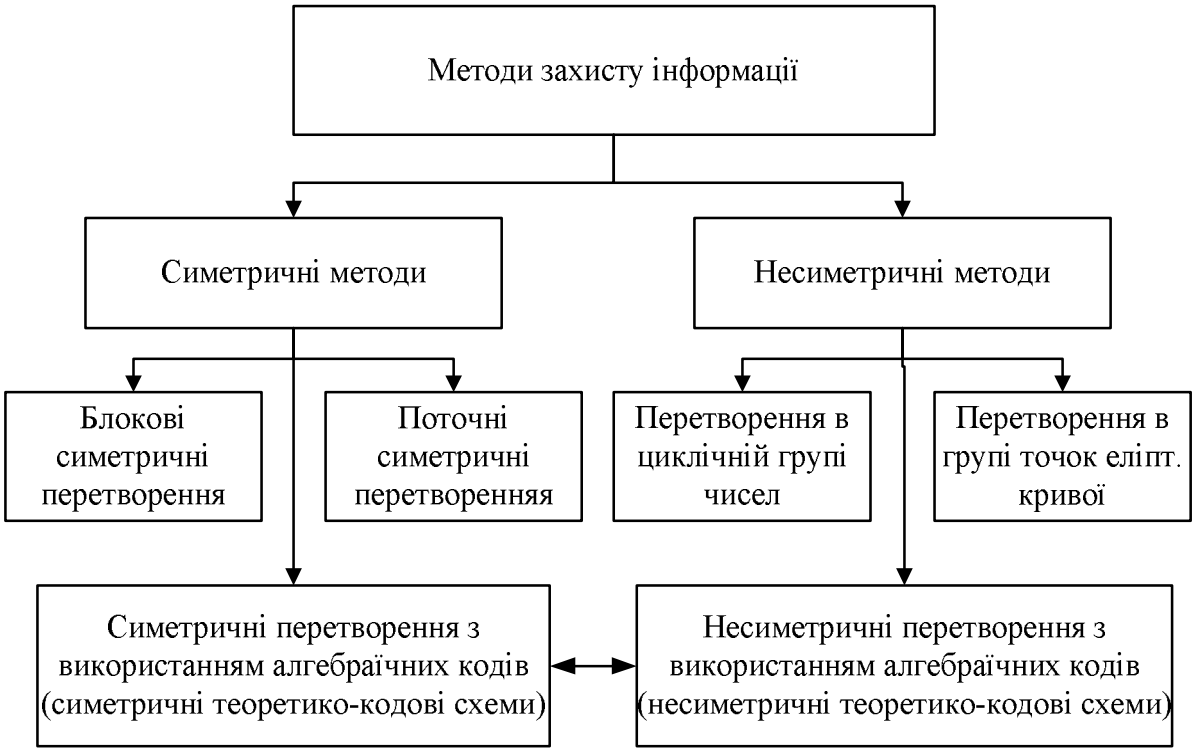

Рис. 1. Загальна класифікація криптографічних методів захисту інформації

Перспективним напрямом в розвитку криптографічних засобів захисту інформації доказової стійкості є крипто-кодові механізми, побудова яких заснована на зведенні завдання злому ключових даних до розв'язання теоретико-числової задачі декодування випадкового коду [7-11]. У деяких джерелах вони отримали назву теоретико-кодових схем (ТКС)[9-10].

Як показує проведений аналіз їх застосування дозволяє реалізувати швидке криптографічне перетворення із забезпеченням доказової стійкості (див. табл. 1.). Складність їх реалізації порівнювальна з симетричними криптоалгоритмами (блоково-симетричними шифрами (БСШ)). Крім того, їх практичне використання дозволяє застосувати інфраструктуру відкритих ключів і будувати інтегровані механізми криптографічного перетворення даних і канального кодування для комплексного забезпечення безпеки і достовірності передачі даних.

В таблиці. 1. приведені результати порівняльних досліджень ефективності криптографічних методів захисту інформації при фіксованому рівні стійкості:

- середньому (складність криптоаналізу найкращим відомим алгоритмом не менше 2^{128} операцій);
- високому (складність криптоаналізу найкращим відомим алгоритмом не менше 2^{256} операцій);
- надвисокому (складність криптоаналізу найкращим відомим алгоритмом не менше 2^{512} операцій).

Таблиця 1.

Результати порівняльних досліджень ефективності криптографічних методів захисту інформації при фіксованому рівні стійкості

Методи криптографічного перетворення	Модель безпеки	Довжина ключових даних, біт	Швидкість крипт. перетв., біт/с	Додаткові функції
Блочні симетричні шифри	Практична безпека	128, 256,	$10^6 – 10^9$	Так

		512		
Поточні симетричні шифри	Практична безпека	128, 256, 512	$10^7 – 10^{10}$	Так
Несиметричні RSA-подібні криптоалгоритми	Доказова безпека	3248 (128), 15424 (256)	$10^2 – 10^3$	Так
Несиметричні криптоалгоритми на еліптичних кривих	Доказова безпека	283 (128), 571 (256)	$10^3 – 10^4$	Так
Несиметричні криптоалгоритми з використанням кодових конструкцій	Доказова безпека	$0{,}5 \cdot 10^6$ (128), $2 \cdot 10^6$ (256)	$10^6 – 10^8$	Контроль помилок, підвищення достовірності

У другій колонці таблиці приведена відповідна модель безпеки, по загальноєвропейській класифікації (див. звіт про криптографічний конкурс NESSIE). У третій колонці приведена відповідна заявленому рівню стійкості мінімальна довжина ключових даних криптоалгоритму. Для несиметричних криптоалгоритмів в дужках вказана еквівалентна (по стійкості) довжина ключів симетричних криптоалгоритмів. У четвертій колонці таблиці приведені оцінки швидкодії криптоалгоритму, тобто оцінки швидкості криптографічного перетворення інформації.

До додаткових функцій криптоалгоритмів (див. останню колонку таблиці) слід віднести можливість виявлення і/або виправлення помилок, що виникають при передачі даних по каналах зв'язку. Ця функція дозволяє реалізувати комплексне забезпечення безпеки і достовірності передачі даних в комп'ютерних системах і мережах. Як випливає з приведених в таблицю 1 даних, подібну можливість можуть надавати тільки криптоалгоритми, засновані на використанні кодових конструкцій (крипто-кодові засоби захисту інформації). Вони будуються шляхом маскування (приховування в таємниці) від зловмисника швидкого правила декодування (поліноміальній складності) кодових слів, внаслідок чого не уповноважена особа без знання секретного ключа вимушена використовувати складні алгоритми переборного пошуку (у загальному випадку експоненціальної складності) для декодування отриманої послідовності.

Таким чином, як випливає з приведених результатів порівняльного аналізу, несиметричні криптоалгоритми з використанням кодових конструкцій дозволяють реалізувати криптографічний захист інформації за технологією відкритих ключів. Швидкість крипто-кодового перетворення інформації порівнювальна із швидкістю шифрування (розшифрування) блоковими симетричними шифрами. Крім того в роботах [10-12] показано, що практичне використання крипто-кодових засобів захисту інформації дозволяє на основі інтеграції механізмів канального кодування і шифрування комплексно забезпечити безпеку і достовірність даних, які передаються. Отже, застосування теоретико-кодових схем з одного боку економічно вигідніше за застосування цілого комплексу різних механізмів шифрування і канального кодування, які вирішують окремо узяті завдання, а з іншого - спостерігається істотне зниження сумарних обчислювальних витрат, що приходяться на одиницю інформації, яка оброблюється і передається, тобто за рахунок зниження часу обробки підвищується оперативність передачі даних.

Загальна класифікація відомих методів побудови теоретико-кодових схем приведена на рис. 2.

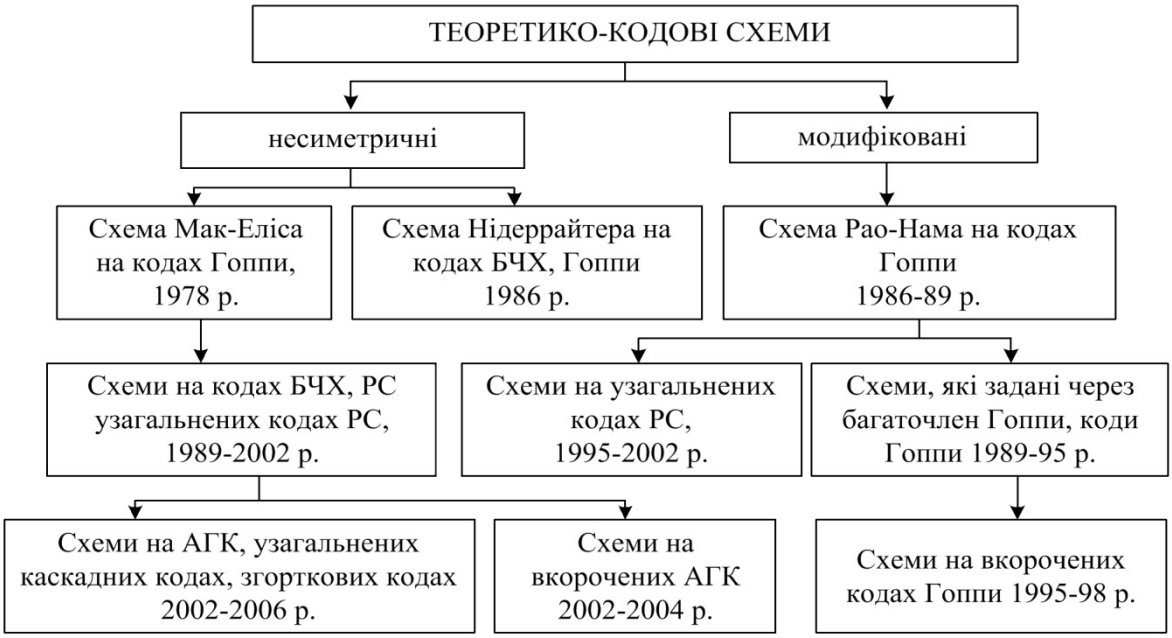

Рис. 2. Загальна класифікація теоретико-кодових схем

Проведений аналіз і порівняльні дослідження показали, що відомі несиметричні крипто-кодові засоби захисту інформації будуються за двома схемами: з маскуванням породжуючої матриці коду (схема Мак-Еліса), і з маскуванням перевірочної матриці коду (схема Нідеррайтера)[7, 8]. Симетрична схема Рао-Нама по суті є деяким спрощенням несиметричної конструкції Мак-Еліса. Початковими об'єктами можуть виступати алгебраїчні блокові коди з швидким (поліноміальної складності) алгоритмом декодування, такі, наприклад, як коди Гоппи, Ріда-Соломона (РС), Боуза-Чоудхурі-Хоквігнема (БЧХ) [7-11].

Найбільш ефективними по стійкості до алгоритмів криптоаналізу являються крипто-кодові засоби захисту інформації з недвійковими лінійними блоковими кодами, що виникають на алгебраїчних кривих, - алгеброгеометричними кодами (АГК) [10-11]. З одного боку, подібні конструкції стійкі до атак, які запропоновані Сідельніковим [9], з іншого боку, вони забезпечують високі показники достовірності і оперативності передачі даних [10-12]. Практичне використання крипто-кодових засобів захисту інформації з недвійковими алгебраїчними блоковими кодами припускає застосування методів і обчислювальних алгоритмів недвійкового рівновагового кодування (як за схемою Мак-Еліса, так і за схемою Ніддеррайтера). На сьогодні, виходячи з проведеного аналізу наукових робіт і публікацій в періодичних виданнях [12-14] витікає, що методи рівновагового кодування розроблені тільки на випадок двійкових кодових послідовностей, тобто існуючий науково-методичний апарат, застосовувані методи і обчислювальні алгоритми не дозволяють реалізувати недвійкове рівновагове кодування, у тому числі і в крипто-кодових засобах захисту інформації.

Таким чином, актуальним науково-технічним завданням, що має важливе прикладне значення в області побудови обчислювально ефективних криптографічних засобів захисту інформації, є розробка методів і алгоритмів недвійкового рівновагового кодування і крипто-кодових засобів на їх основі для комплексного забезпечення безпеки і достовірності передачі даних в комп'ютерних системах і мережах. Їх застосування дозволить:

- реалізувати швидкі криптографічні перетворення великих об'ємів даних з використанням відкритих ключів в комп'ютерних системах і мережах;
- забезпечити високий рівень стійкості до сучасних методів криптоаналізу, за рахунок зведення завдання безключового читання до розвязання теоретико-складної задачі декодування випадкового коду забезпечити доказову стійкість криптографічних засобів захисту інформації;
- будувати на канальному рівні еталонної моделі взаємодії відкритих мереж інтегровані механізми криптографічного захисту інформації і достовірності даних в комп'ютерних системах і мережах.

Таким чином, рішення важливого науково-технічного завдання, що полягає в розробці методу побудови криптосистем доказової стійкості на алгебраїчних блокових кодах для криптографічного захисту інформації в комп'ютерних системах і мережах, є актуальним.

Висновки. Проведений аналіз показує, що існуючі нессиметричні криптографічні засоби захисту інформації не забезпечують сучасних вимог: складність реалізації криптографічних перетворень на 3 - 5 порядків вища, ніж у аналогічних симетричних систем (блоково-симетричних шифрів), що в умовах стрімкого збільшення об'ємів даних, які оброблюються і передаються неприпустимо. Істотними недоліками несиметричних криптографічних засобів захисту інформації є їх неспроможність в реалізації швидких криптоперетворень великих об'ємів даних з використанням інфраструктури відкритих ключів. Крім того, застосування симетричних криптографічних засобів захисту інформації припускає наявність дорогої інфраструктури формування, зберігання, поширення і утилізації секретних ключових даних, що для більшості комп'ютерних систем і мереж є неприйнятною умовою.

Таким чином, в результаті проведених досліджень виявлено об'єктивно існуюче протиріччя між зростанням об'ємів інформації, які підлягають несиметричному криптографічному перетворенню із забезпеченням доказової стійкості, і лімітом часу для обробки інформації криптографічними засобами захисту. Потрібна наукова розробка нових методів, алгоритмів і технічних засобів на їх основі для ефективного криптографічного захисту інформації з високими показниками безпеки, яка забезпечується, достовірності і оперативності передачі даних і можливістю застосування технології відкритих ключів. Найбільш перспективним напрямом в цьому сенсі є крипто-кодові засоби захисту інформації, які дозволяють на основі інтеграції механізмів канального кодування і шифрування комплексно забезпечувати безпеку і достовірність даних, які передаються. В зв'язку з цим, перспективним напрямом подальших досліджень є розробка і подальше вдосконалення крипто-кодових засобів захисту інформації і протоколів обміну секретними повідомленнями в різних режимах функціонування комп'ютерних систем і мереж.

Список літератури

1. Захист інформації в комп’ютерних системах від несанкціонованого доступу. / За ред. С.Г. Лаптєва. – К., 2001. – 321 с.
2. Мамаев Е. Технологии защиты информации в Интернете. – СПб.: ИД Питер, 2001. – 848 с.
3. Харин Ю.С. Берник В.И., Матвеев Г.В., Агиевич С.В. Математические и компьютерные основы криптологии. – Мн.: Новое знание, 2003. – 382 с.
4. Мао В. Современная криптография. Теория и практика. – М.: «Вильямс», 2005. – 768с.
5. Шнайер Б. Прикладная криптография. –М.: «ТРИУМФ», 2003. – 816 с.
6. Молдавян Н.А., Молдавян А.А., Еремееев М.А. Криптография: от примитивов к синтезу алгоритмов. – СПб.: БХВ, 2004. – 448 с.
7. R.J. McEliece. A Public-Key Criptosystem Based on Algebraic Theory. // DGN Progres Report 42-44, Jet Propulsi on Lab. Pasadena, CA. January – February, 1978. – P. 114-116.
8. H. Niederreiter. Knapsack-Type Cryptosystems and Algebraic Coding Theory. // Probl. Control and Inform. Theory. – 1986. –V.15. – P. 19-34.
9. Сидельников В.М. Криптография и теория кодирования. Материалы конференции «Московский университет и развитие криптографии в России», МГУ. – 2002. – 22с.
10. Стасев Ю.В., Кузнецов А.А. Несимметричные теоретико-кодовые схемы с использованием алгеброгеометрических кодов. // Кибернетика и системный анализ: Международный научно-теоретический журнал. – Киев: НАНУ. – 2005. – №3. – С. 47-57.
11. Кузнецов А.А. Несимметричные криптосистемы доказуемой стойкости на алгебраических блоковых кодах // Радіоелектронні і комп’ютерні системи. Науково-технічний журнал – Х.: ХАИ. – 2007.– №8(27) – С.130-144.
12. Науменко Н. І., Стасев Ю. В., Кузнецов О.О.Теоретичні основи та методи побудови алгебраїчних блокових кодів. Х.:ХУ ПС, 2005р. – 267с.
13. Кларк Дж.-мл., Кейн Дж. Кодирование с исправлением ошибок в системах цифровой связи: Пер. с англ. / Под ред. Б.С. Цыбакова. – М.: Радио и связь, 1987. – 392 с.
14. Блейхут Р. Теория и практика кодов, контролирующих ошибки: Пер. с англ. – М.: Мир, 1986. –576 с.

Рецензент: д.т.н., проф. Хорошко В.О.
Надійшла 25.02.2010 р.